KESSLER TOPAZ
MELTZER & CHECK, LLP
ELI R. GREENSTEIN (Bar No. 217945)
egreenstein@ktmc.com
JENNIFER L. JOOST (Bar No. 296164)
jjoost@ktmc.com
STACEY M. KAPLAN (Bar No. 241989)
skaplan@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Tel: (415) 400-3000
Fax: (415) 400-3001

Attorneys for Plaintiff Zog, Inc.
[additional counsel listed on signature page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

ZOG, INC., Individually and on Behalf of All Others Similarly Situated,

Plaintiff,

v.

INTEL CORPORATION,

Defendant.

Civil Action No._____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Zog, Inc. ("Plaintiff"), on behalf of itself and all others similarly situated, hereby alleges the following based on personal knowledge as to itself and its own conduct, and upon information and belief as to all other matters.

I. INTRODUCTION

1. Defendant Intel Corporation ("Defendant" or "Intel") is one of the largest manufacturers of central processing units ("CPUs" or "processors"). Intel's processors are integrated—with Intel's assistance and guidance—into desktop and laptop computers, servers, and smartphones manufactured by, *inter alia*, Dell Inc., Lenovo Group Limited, HP Inc., Acer Inc., and Apple Inc.

2. Given that CPUs are responsible for executing instructions provided by various software programs, the processing speed of a CPU is critical to running software programs effectively and efficiently. Likewise, a CPU's ability to securely process data is critical to maintaining the integrity of a user's confidential and sensitive information.

3. To this end, Intel has long touted the purported speed and security of its processors in marketing materials directed to business and enterprise customers. For example, when launching its 7th Gen Core vPro processor in January 2017, Intel emphasized that the new processor delivered a "best-in-class platform for business that arms IT pros with the most advanced set of capabilities across the areas they care about – security, productivity, and manageability."[1]

4. However, unbeknownst to Plaintiff and members of the Class (defined herein), Intel's processors are defective. Specifically, Intel processors are incapable of operating at represented processing speeds without exposing users to two security vulnerabilities (the "Defects")—known as "Meltdown" and "Spectre"—which "allow programs to steal data which is currently processed on the computer."[2] "Although both [Defects] are based on the same general principle, Meltdown allows

---

[1] Tom Garrison, *7th Gen Intel Core vPro Processors: New Levels of Performance, Security and Manageability for Businesses*, INTEL CORPORATION, January 3, 2017, https://itpeernetwork.intel.com/7th-gen-intel-core-vpro-business-performance-security-manageability/ (last accessed January 12, 2018).

[2] Graz University of Technology, *Meltdown and Spectre*, https://meltdownattack.com/ (last accessed January 12, 2018).

malicious programs to gain access to higher-privileged parts of a computer's memory, while Spectre steals data from the memory of other applications running on a machine."[3]

5. After the Defects were publicly revealed by *The Register* on January 2, 2018,[4] it was reported that Intel had known about the Spectre Defect since ***at the latest*** June 1, 2017, and the Meltdown Defect since ***at the latest*** July 28, 2017.[5] Notwithstanding Intel's knowledge of the Defects—and the fact that Intel should have known of the Defects many years ago—Intel continued to advertise, manufacture, distribute, and sell the defective processors to members of the Class including Plaintiff.

6. The Defects are present in virtually every modern Intel processor and cannot be effectively fixed through software "patches" or updates. In fact, efforts to mitigate the Defects—which "impact fundamental aspects of how mainstream processors manage and silo data"—have resulted in "corresponding performance slowdowns" given that "the fixes involve routing data for processing in less efficient ways."[6]

7. Initial estimates have suggested that software patches intended to mitigate the Defects may reduce processing speed by as much as thirty percent[7]—a concern reinforced by Intel's confirmation that patched personal computers have shown a "2 percent to 14 percent" decline in

---

[3] Andy Greenberg, *A Critical Intel Flaw Breaks Basic Security for Most Computers*, WIRED, January 3, 2018, https://www.wired.com/story/critical-intel-flaw-breaks-basic-security-for-most-computers/ (last accessed January 12, 2018).

[4] *See* John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor Design Flaw Forces Linux, Windows Redesign*, THE REGISTER, January 2, 2018, https://www.theregister.co.uk/2018/01/02/intel_cpu_design_flaw/ (last accessed January 12, 2018).

[5] *See* Samuel Gibbs, *Meltdown and Spectre: 'Worst Ever' CPU Bugs Affect Virtually All Computers*, THE GUARDIAN, January 4, 2018, https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw (last accessed January 12, 2018) ("Google said it informed the affected companies about the Spectre flaw on 1 June 2017 and later reported the Meltdown flaw before 28 July 2017.").

[6] Lily Hay Newman, *Meltdown and Spectre Fixes Arrive—But Don't Solve Everything*, WIRED, January 6, 2018, https://www.wired.com/story/meltdown-and-spectre-vulnerability-fix/ (last accessed January 12, 2018).

[7] *See* John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor Design Flaw Forces Linux, Windows Redesign*, THE REGISTER, January 2, 2018.

performance speed[8] and Microsoft Corp.'s confirmation that Meltdown-related patches for computers and servers running Windows operating systems with Intel processors result in potentially significant slowdowns.[9]

8. The Defects are of significant risks to businesses given the devastating implications of a cyber-attack on a business's ability to function. Indeed, "[t]he U.S' National Cyber Security Alliance found that 60 percent of small companies are unable to sustain their businesses over six months after a cyber attack. According to the Ponemon Institute, the average price for small businesses to clean up after their businesses have been hacked stands at $690,000; and, for middle market companies, it's over $1 million."[10]

9. Plaintiff and members of the Class would not have purchased or leased—or would have paid substantially less for—Intel processors (or devices containing Intel processors) had they known of the Defects and the reduction in processing performance associated with efforts necessary to mitigate the substantial security risks presented by the Defects.

10. Defendant's conduct violates state common law and statutory law.

11. Accordingly, Plaintiff brings this class action against Defendant individually and on behalf of all other persons and entities in the United States that purchased or leased one or more Intel processors, or one or more devices containing an Intel processor, for business or commercial use.

II. PARTIES

12. Plaintiff Zog, Inc. is incorporated and headquartered in the Commonwealth of Pennsylvania. Plaintiff provides information technology management, maintenance, and support services to other businesses and enterprises, including the provision of secure cloud services. Plaintiff purchased numerous devices containing Intel processors including, for example:

---

[8] Intel Corporation, *Intel Offers Security Issue Update*, January 9, 2018, https://newsroom.intel.com/news/intel-offers-security-issue-update/ (last accessed January 12, 2018).

[9] Terry Myerson, *Understanding the Performance Impact of Spectre and Meltdown Mitigations on Windows Systems*, MICROSOFT CORP., January 9, 2018, https://cloudblogs.microsoft.com/microsoftsecure/2018/01/09/understanding-the-performance-impact-of-spectre-and-meltdown-mitigations-on-windows-systems/ (last accessed January 12, 2018).

[10] Gary Miller, *60% of Small Companies That Suffer A Cyber Attack Are Out Of Business Within Six Months*, THE DENVER POST, October 23, 2016.

- one HP ProBook 440 G4 14" Notebook, containing an Intel Core i3-7100U processor, for $554 on September 27, 2017;
- one HP Business Desktop ProDesk 600 G2 Desktop Computer, containing an Intel Core i5-6500 processor, for $679 on January 18, 2017;
- one HPE (Hewlett Packard Enterprise) ML350T09 Smart Buy Server, containing an Intel Xeon E5-2640 v4 processor, for $2339 on January 5, 2017; and
- one Intel Xeon E5-2640 v4 processor for $993 on January 5, 2017.

13. Defendant Intel Corporation is a Delaware corporation with its principal place of business located within this District at 2200 Mission College Boulevard, Santa Clara, California. Defendant is engaged in the business of designing, manufacturing, selling, and/or distributing CPUs, including the defective processors at issue here. All references herein to any act of Intel shall include the acts of Intel's directors, officers, employees, affiliates, subsidiaries, and agents where such persons or entities were engaged in the management, direction, or control of Intel, or where such persons or entities were acting act the direction of Intel.

III. JURISDICTION AND VENUE

14. This Court has general personal jurisdiction over Defendant because it resides within this District.

15. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d) because this matter is a putative class action, the Class contains members, including Plaintiff, that are citizens of a state different from Defendant, there are more than 100 members of the Class, and the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000.

16. Venue properly lies in this District pursuant to 28 U.S.C. § 1391 because Defendant maintains its principal place of business in this District, a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and because Defendant conducts a substantial amount of business in this District.

17. Assignment to the San Jose Division of this District is proper under Northern District of California Civil Local Rule 3-2(c) because a substantial part of the events or omissions which give rise to Plaintiff's claims occurred, and Defendant's principal place of business is located, in Santa

Clara, California. Pursuant to Northern District of California Civil Local Rule 3-2(e), all civil actions which arise in the Santa Clara County shall be assigned to the San Jose Division.

IV. FACTUAL ALLEGATIONS

18. Intel is one of the world's largest manufacturers of CPUs—the so-called "brains" of computer systems (and other electronic devices)—which are responsible for processing system data and controlling other devices and components connected to the system.

19. Intel both sells its processors to the marketplace as stand-alone components and sells its processors to third-party manufacturers that—with Intel's assistance and guidance—incorporate Intel's processors into, among other things, desktop and laptop computers, servers, and smartphones. Third-party manufacturers utilizing Intel processors include household names such as Dell Inc., Lenovo Group Limited, HP Inc., Acer Inc., and Apple Inc.

20. Fundamental to the operation of a CPU is the operating system's "kernel"—the program responsible for directing and coordinating access to the CPU, random-access memory, and other components such as keyboards, mice, disk-drives, printers, and monitors. In order to ensure effective performance and maintain security, the kernel is responsible for preventing data associated with one program from being accessed or overwritten by another program.

A. Intel Touts the Processing Speed and Security of Its Processors

21. Processing speed and security are two of the key attributes of CPUs. Without sufficient processing speed, a CPU will be unable to effectively and efficiently run the computer's operating system and software programs, and utilize connected hardware and peripheral devices. Similarly, without sufficient data security, a CPU will not be able to satisfy users' needs for the processing, communication, and storage of sensitive and confidential information.

22. Given these market demands, Intel has consistently touted the purported speed and security of its processors in communications with its prospective business and enterprise customers. For example, when Intel launched its 7th Gen Core vPro processor in January 2017, Intel touted the processor's "new levels of performance, security and manageability for business" and specifically represented that the new processor delivered a "best-in-class platform for business that arms IT pros with the most advanced set of capabilities across the areas they care about – security, productivity,

and manageability."[11] Furthermore, Intel assured customers that "[w]ith [the] 7th Gen Core vPro processor, [Intel's] focus is to deliver customers the solutions they need to fight against identity and data breaches."[12] Ultimately, Intel claimed that "upgrading to Windows 10 and 7th Gen Core vPro processor-based devices will put enterprises on the best path to safeguard identities, drive down costs while future-proofing their business."[13]

23. Similarly, in advertising materials for server boards equipped with Xeon-brand processors, Intel represented that "[e]very Intel® Server Board is designed and engineered to deliver the performance, reliability and security customers need with the quality and support they have come to expect from Intel."[14] Likewise, Intel touted "the broader benefits provided by the Intel Xeon Platinum processor, which is designed for scalability, security, performance, and to take businesses into the future."[15]

24. In addition to these product-line representations, Intel specifically markets each model of its processors based on their respective processing speeds. For example, Intel's website allows prospective customers to directly and easily compare the processing speed (or "clock speed") of each of its processors:[16]

---

[11] Tom Garrison, *7th Gen Intel Core vPro Processors: New Levels of Performance, Security and Manageability for Businesses*, INTEL CORPORATION, January 3, 2017.

[12] *Id*.

[13] *Id*.

[14] Intel Corporation, *Intel Server Boards*, https://www.intel.com/content/www/us/en/motherboards/server-motherboards/server-board.html (last accessed January 12, 2018).

[15] Tim Allen, *The Intel Xeon Platinum Processor Is Put to the Test and Comes Out Shining*, INTEL CORPORATION, July 11, 2017, https://itpeernetwork.intel.com/intel-xeon-platinum-processor-put-to-test/ (last accessed January 12, 2018).

[16] *See* Intel Corporation, *Intel® Xeon® Processor E5-2640 v4*, https://www.intel.com/content/www/us/en/products/processors/xeon/e5-processors/e5-2640-v4.html (last accessed January 12, 2018); Intel Corporation, Intel® Core™ i3-7100U Processor, https://www.intel.com/content/www/us/en/products/processors/core/i3-processors/i3-7100u.html (last accessed January 12, 2018).

B. The Defects

25. Rather than processing instructions in sequential order, Intel CPUs are designed to process multiple program instructions in parallel through so-called "out-of-order" or "speculative" execution.

26. As explained by the team of researchers from the Graz University of Technology that helped identify the Defects:

> Speculative execution is a technique used by highspeed processors in order to increase performance by guessing likely future execution paths and prematurely executing the instructions in them. For example when the program's control flow depends on an uncached value located in the physical memory, it may take several hundred clock cycles before the value becomes known. Rather than wasting these cycles by idling, the processor guesses the direction of control flow, saves a checkpoint of its register state, and proceeds to speculatively execute the program on the guessed path. When the value eventually arrives from memory the processor checks the correctness of its initial guess. If the guess was wrong, the processor discards the (incorrect) speculative execution by reverting the register state back to the stored checkpoint, resulting in performance comparable to idling. In case the guess was correct, however, the speculative execution results are committed, yielding a

> significant performance gain as useful work was accomplished during the delay.[17]

27. As first reported by *The Register* on January 2, 2018, because "Intel's CPUs speculatively execute code potentially without performing security checks . . . it may be possible to craft software in such a way that the processor starts executing an instruction that would normally be blocked – such as reading kernel memory from user mode – and completes that instruction before the privilege level check occurs."[18]

28. Stated differently, "malicious actors c[an] take advantage of speculative execution to read system memory that should have been inaccessible" and may, as a result, be able to "read sensitive information in the system's memory such as passwords, encryption keys, or sensitive information open in applications" through two similar security vulnerabilities known as "Meltdown" and "Spectre."[19]

The Meltdown Defect

29. As explained by the Graz University team, "Meltdown breaks the most fundamental isolation between user applications and the operating system" and "allows a program to access the memory, and thus also the secrets, of other programs and the operating system."[20] As a result, the Meltdown Defect "enables an adversary to read memory of other processes or virtual machines in the cloud without any permissions or privileges, affecting millions of customers and virtually every user of a personal computer."[21]

---

[17] Paul Kocher, *et al.*, *Spectre Attacks: Exploiting Speculative Execution*∗, https://spectreattack.com/spectre.pdf (last accessed January 11, 2018) (the "Spectre White Paper").

[18] John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor Design Flaw Forces Linux, Windows Redesign*, THE REGISTER, January 2, 2018.

[19] Matt Linton, *Today's CPU Vulnerability: What You Need to Know*, GOOGLE SECURITY BLOG, January 3, 2018, https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html (last accessed January 12, 2018).

[20] Graz University of Technology, *Meltdown and Spectre*.

[21] Moritz Lipp, *et al.*, *Meltdown*, https://meltdownattack.com/meltdown.pdf (last accessed January 11, 2018) (the "Meltdown White Paper"); *see also* Matt Linton, *Today's CPU Vulnerability: What You Need to Know*, GOOGLE SECURITY BLOG, January 3, 2018 ("Testing also showed that an attack running on one virtual machine was able to access the physical memory of the host machine, and through that, gain read-access to the memory of a different virtual machine on the same host.").

30. While other modern processor manufacturers utilize speculative execution, the Meltdown Defect is unique to Intel's processor given the "particularly aggressive way" in which Intel processors "perform speculation around memory accesses."[22] As explained by *Ars Technica*:

> Operating system memory has associated metadata that determines whether it can be accessed from user programs or is restricted to access from the kernel. . . . Intel chips allow user programs to speculatively use kernel data, and the access check (to see if the kernel memory is accessible to a user program) happens some time *after* the instruction starts executing. . . . With careful timing, this can be used [by a malicious actor] to infer the values stored in kernel memory.[23]

31. While Intel and its business partners have started offering firmware and software patches designed to mitigate the Meltdown Defect, these "fixes" are wholly inadequate given that they substantially reduce processing speed. Indeed, because the patches have been designed to prevent shared access to kernel memory—such that malicious actors cannot access sensitive data stored in the kernel memory—the patches "make[] every single call into the kernel a bit slower, because each switch to the kernel now requires the kernel page to be reloaded."[24]

32. As *The Register* explained in greater detail:

> The fix is to separate the kernel's memory completely from user processes using what's called Kernel Page Table Isolation, or KPTI.
>
> * * *
>
> Whenever a running program needs to do anything useful—such as write to a file or open a network connection—it has to temporarily hand control of the processor to the kernel to carry out the job. To make the transition from user mode to kernel mode and back to user mode as fast and efficient as possible, the kernel is present in all processes' virtual memory address spaces, although it is invisible to these programs. When the kernel is needed, the program makes a system call, the processor switches to kernel mode and enters the kernel. When it is done, the CPU is told to switch back to user mode, and reenter the

---

[22] Peter Bright, *"Meltdown" and "Spectre": Every Modern Processor Has Unfixable Security Flaws*, ARS TECHNICA, January 3, 2018, https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-every-modern-processor-has-unfixable-security-flaws/ (last accessed January 12, 2018).

[23] *Id*.

[24] *Id*. (emphasis in original).

> process. While in user mode, the kernel's code and data remains out of sight but present in the process's page tables.
>
> Think of the kernel as God sitting on a cloud, looking down on Earth. It's there, and no normal being can see it, yet they can pray to it.
>
> These KPTI patches move the kernel into a completely separate address space, so it's not just invisible to a running process, it's not even there at all. Really, this shouldn't be needed, but clearly there is a flaw in Intel's silicon that allows kernel access protections to be bypassed in some way.
>
> The downside to this separation is that it is relatively expensive, time wise, to keep switching between two separate address spaces for every system call and for every interrupt from the hardware. These context switches do not happen instantly, and they force the processor to dump cached data and reload information from memory. This increases the kernel's overheard, and slows down the computer.
>
> Your Intel-powered machines will run slower as a result.[25]

33. Indeed, researchers have estimated that the software patches designed to mitigate the Meltdown Defect may reduce processing speed by as much as thirty percent.[26] In fact, Intel has admitted that patched personal computers have shown a "2 percent to 14 percent" decline in performance speed in Defendant's own testing.[27] More recent benchmark testing by Microsoft Corp. has confirmed that Meltdown patches for computers and servers running Windows operating systems with Intel processors result in potentially significant slowdowns.[28]

34. Further, experts have noted that the rush to roll out patches, while necessary, makes the ultimate efficacy of these early fixes potentially suspect, as there has not been much time for

---

[25] John Leyden and Chris Williams, *Kernel-memory-leaking Intel Processor Design Flaw Forces Linux, Windows Redesign*, THE REGISTER, January 2, 2018.

[26] *See, e.g.*, *id.*

[27] Intel Corporation, *Intel Offers Security Issue Update*, January 9, 2018.

[28] Terry Myerson, *Understanding the Performance Impact of Spectre and Meltdown Mitigations on Windows Systems*, MICROSOFT CORP., January 9, 2018.

extensive testing and refinement. Thus, these "slapdash fixes" may not offer total protection, or could create other bugs and instabilities that will need to be resolved.[29]

35. In fact, on January 11, 2018, it was reported that Intel's "patches had bugs of their own" and that Intel was "advis[ing] customers to 'delay additional deployments of these microcode updates.'"[30] As explained by Paul Kocher, one of the researchers who identified the Defects, "[i]t doesn't surprise me a lot that there would be some hiccups."[31]

The Spectre Defect

36. Like the Meltdown Defect, the Spectre Defect takes advantage of design defects in Intel processors' use of speculative execution.

37. The research team from Graz University has explained that "Spectre breaks the isolation between different applications" and "allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets."[32]

38. More specifically, "Spectre attacks involve inducing a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim's confidential information via a side channel to the adversary."[33] For example, a Spectre attack can "leak information within a browser (such as saved passwords or cookies) to a malicious JavaScript"—which, in turn, sends the passwords or cookies back to the malicious actor.[34]

---

[29] Lily Hay Newman, *Meltdown and Spectre Fixes Arrive—But Don't Solve Everything*, WIRED, January 6, 2018.

[30] Robert McMillan, *Intel Fumbles Its Patch for Chip Flaw*, THE WALL STREET JOURNAL, January 11, 2018, https://arstechnica.com/gadgets/2018/01/heres-how-and-why-the-spectre-and-meltdown-patches-will-hurt-performance/ (last accessed January 12, 2018).

[31] *Id*.

[32] Graz University of Technology, *Meltdown and Spectre*, https://spectreattack.com/ (last accessed January 12, 2018).

[33] Spectre White Paper.

[34] Peter Bright, *Here's How, and Why, the Spectre and Meltdown Patches Will Hurt Performance*, ARS TECHNICA, January 11, 2018, https://arstechnica.com/gadgets/2018/01/heres-how-and-why-the-spectre-and-meltdown-patches-will-hurt-performance/ (last accessed January 12, 2018).

39. To date, at least two particular types of Spectre attacks have emerged: "[o]ne version [the "branch prediction variant"] allows an attacker to 'train' the processor's branch prediction machinery so that a victim process mispredicts and speculatively executes code of an attacker's choosing (with measurable side-effects); the other [the "array bounds variant"] tricks the processor into making speculative accesses outside the bounds of an array."[35]

40. Fixing the Spectre Defect is particularly complicated. As explained by *Ars Technica*:

> while there may be limited ways to block certain kinds of speculative execution, general techniques that will defend against any information leakage due to speculative execution aren't known.
>
> Sensitive pieces of code could be amended to include 'serializing instructions'—instructions that force the processor to wait for all outstanding memory reads and writes to finish (and hence prevent any speculation based on those reads and writes)—that prevent most kinds of speculation from occurring. . . . But these instructions would have to be very carefully placed, with no easy way of identifying the correct placement.[36]

As such, "at-risk applications (notably, browsers) are being updated to include certain Spectre mitigating techniques to guard against the array bounds variant" while "[o]perating system and processor updates are needed to address the branch prediction version."[37]

C. Defendant's Knowledge of the Defects

41. Although the public only became aware of the Defects in Intel processors in January 2018, Intel has been aware of the Spectre Defect since ***at the latest*** June 1, 2017, and the Meltdown Defect since ***at the latest*** July 28, 2017, when a team from Google's Project Zero alerted the company to the existence of the Defects.[38] In fact, in the intervening months between Google's discovery and

---

[35] *Id.*

[36] Peter Bright, *"Meltdown" and "Spectre": Every Modern Processor Has Unfixable Security Flaws*, ARS TECHNICA, January 3, 2018.

[37] Peter Bright, *Here's How, and Why, the Spectre and Meltdown Patches Will Hurt Performance*, ARS TECHNICA, January 11, 2018.

[38] *See* Samuel Gibbs, *Meltdown and Spectre: 'Worst Ever' CPU Bugs Affect Virtually All Computers*, THE GUARDIAN, January 4, 2018, https://www.theguardian.com/technology/2018/jan/04/meltdown-spectre-worst-cpu-bugs-ever-found-affect-computers-intel-processors-security-flaw (last accessed January 12, 2018) ("Google said it informed the affected companies about the Spectre flaw on 1 June 2017 and later reported the Meltdown flaw before 28 July 2017.").

The Register's report, at least three other outside research teams alerted Intel to the existence of the Defects.[39]

42. Intel knew, or should have known, of the Defect in its processors many years ago given that Intel was in a superior position to perform proper tests and security checks of its processors and appropriate due diligence would have revealed the vulnerabilities that were uncovered by various independent teams. Indeed, Defendant had actual knowledge, and access to proprietary information to discover, that defects in design were causing the Defects in its processors.

43. As stated succinctly by Paul Kocher, "[t]here's no reason someone couldn't have found this years ago instead of today."[40]

44. Indeed, warning signs have existed since at least early 2005 when "[r]esearchers began writing about the potential for security weaknesses at the heart of central processing units."[41] This influential work continued in 2013 when "other research papers showed that CPUs let unauthorized users see the layout of the kernel, a set of instructions that guide how computers perform key tasks like managing files and security and allocating resources."[42]

45. These early reports ultimately prompted industry presentations at various "Black Hat" and other cybersecurity conferences in 2016 and 2017, including presentations by members of the Graz University team, regarding potential attacks against the kernel memory of Intel processors.[43]

46. Nevertheless, rather than inform the public about the Defects, Intel continued to sell its defective processors to unknowing customers at prices much higher than what customers would have paid had they know about the Defects and the impact on processing speeds.

---

[39] Andy Greenberg, *Triple Meltdown: How So Many Researchers Found a 20-Year-Old Chip Flaw At the Same Time*, WIRED, January 7, 2018, https://www.wired.com/story/meltdown-spectre-bug-collision-intel-chip-flaw-discovery/ (last accessed January 12, 2018).

[40] *Id.*

[41] Ian King, *et al.*, *'It Can't Be True': Inside the Semiconductor Industry's Meltdown*, CHICAGO TRIBUNE, January 10, 2018, http://www.chicagotribune.com/bluesky/technology/ct-inside-semiconductor-meltdown-20180110-story.html (last accessed January 12, 2018).

[42] *Id.*

[43] *See id.*

47. As a result, Plaintiff and members of the Class, have been saddled with overpriced processors that are slower and more vulnerable to security risks than what they bargained for.

V. TOLLING OF THE STATUE OF LIMITATIONS AND ESTOPPEL

48. **Discovery Rule Tolling**. Plaintiff and members of the Class could not have reasonably discovered through the exercise of reasonable diligence that their Intel processors suffered from major security vulnerabilities that, if mitigated, resulted in reduced processing performance, within the time period of any applicable statute of limitations.

49. Plaintiff and members of the Class did not discover and did not know of any facts that would have caused a reasonable person to suspect that Defendant was concealing a latent defect and/or that the Intel processors contained a defect that exposed them to security vulnerabilities that, if mitigated, resulted in reduced processing performance.

50. **Fraudulent Concealment Tolling**. Throughout the time period relevant to this action, Defendant concealed from and failed to disclose to Plaintiff and members of the Class vital information concerning the Defects described herein, despite the fact that Defendant knew, or should have known of, the Defects in its Processors well before its discovery by a third party.

51. Defendant kept Plaintiff and members of the Class ignorant of vital information essential to the pursuit of their claims. As a result, neither Plaintiff nor members of the Class could have discovered the Defects, even upon reasonable exercise of diligence.

52. Despite its knowledge of the Defects, Defendant failed to disclose and concealed, and continues to conceal, critical information relating to the Defects from Plaintiff and members of the Class, even though, at any point in time, it could have done so through individual correspondence, media release, or by other means.

53. Plaintiff and members of the Class justifiably relied on Defendant to disclose the Defects in the Intel processors they purchased or leased (either directly or as a component of, among other things, a computer, server, or smartphone), because the Defects were hidden and not discoverable through reasonable efforts by Plaintiff and members of the Class.

54. Thus, the running of all applicable statutes of limitations have been suspended with respect to any claims that Plaintiff and members of the Class have sustained as a result of the defective Intel processors, by virtue of the fraudulent concealment doctrine.

55. **Estoppel**. Defendant was under a continuous duty to disclose to Plaintiff and members of the Class the true character, quality, and nature of the defective processors and associated security vulnerabilities and reductions in processing performance, but concealed the true nature, quality, and character of the processors.

56. Based on the foregoing, Defendant is estopped from relying on any statutes of limitations in defense of this action.

VI. CLASS ACTION ALLEGATIONS

57. Plaintiff brings this proposed action pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and/or 23(b)(3) on behalf of the following Class:

> All persons or entities in the United States that purchased or leased one or more Intel processors, or one or more devices containing an Intel processor, for business or commercial use.

58. Excluded from the Class are Defendant and any parents, subsidiaries, corporate affiliates, officers, directors, employees, assigns, successors, the Court, Court staff, Defendant's counsel, and all respective immediate family members of the excluded entities described above. Plaintiff reserves the right to revise the definition of the Class based upon subsequently discovered information and reserves the right to establish subclasses where appropriate.

59. This action has been brought and may be properly maintained on behalf of the Class proposed herein under Federal Rule of Civil Procedure 23.

60. **Numerosity**. Federal Rule of Civil Procedure 23(a)(1): The Class is so numerous that individual joinder of all potential members is impracticable. Plaintiff believes that there are at least thousands of proposed members of the Class throughout the United States. Members of the Class may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. Mail, electronic mail, Internet postings, and/or published notice.

61. **Commonality and Predominance**. Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3): This action involves common questions of law and fact, which predominate over any questions affecting individual members of the Class, including, without limitation:

A. Whether Defendant engaged in the conduct alleged herein;

B. Whether Defendant's processors are defective and contain the Meltdown Defect and/or the Spectre Defect;

C. Whether the purported "patches," "fixes," or other remedies are ineffective and/or result in reduced processing performance;

D. Whether any such reduced processing performance is material;

E. Whether Defendant knew, or should have known, that its processors were defective and that, if mitigated, resulted reduced processing performance;

F. Whether Defendant had a duty to disclose, and breached its duty to disclose, that its processors were defective and that, if mitigated, resulted in reduced processing performance;

G. Whether Defendant intentionally, recklessly, or negligently misrepresented or omitted material facts including the fact that its processors are defective and that, if mitigated, resulted in reduced processing performance;

H. Whether Defendant breached its express warranties in that its processors were defective with respect to manufacture, workmanship and/or design;

I. Whether Defendant breached its implied warranties in that its processors were defective with respect to manufacture, workmanship and/or design;

J. Whether Defendant was unjustly enriched by the conduct alleged herein;

K. Whether Defendant violated California's Unfair Competition Law, California Business & Professions Code § 17200, *et seq.*;

L. Whether Plaintiff and members of the Class overpaid for Intel Processors;

M. Whether Plaintiff and members of the Class are entitled to equitable relief, including, but not limited to, restitution or injunctive relief; and

N. Whether Plaintiff and members of the Class are entitled to damages and other monetary relief and, if so, in what amount.

62. **Typicality**. Federal Rule of Civil Procedure 23(a)(3): Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all members of the Class were comparably injured through Defendant's wrongful conduct as described above.

63. **Adequacy**. Federal Rule of Civil Procedure 23(a)(4): Plaintiff is an adequate Class representative because its interests do not conflict with the interests of the other members of the Class it seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; and Plaintiff intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and its counsel.

64. **Declaratory and Injunctive Relief**. Federal Rule of Civil Procedure 23(b)(2): Defendant has acted or refused to act on grounds generally applicable to Plaintiff and the other members of the Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Class as a whole.

65. **Superiority**. Federal Rule of Civil Procedure 23(b)(3): A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court

VII. CLAIMS FOR RELIEF

COUNT I

BREACH OF IMPLIED WARRANTY

66. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth herein.

67. Plaintiff brings this count on behalf of itself and the Class.

68. Plaintiff and members of the Class purchased or leased Intel processors, or devices containing Intel processors, from Defendant, by and through Defendant's authorized agents for retail sales, or were otherwise expected to be the eventual purchasers or lessors of Intel processors when purchased or leased from a third party. At all relevant times, Defendant was the manufacturer, distributor, warrantor, and/or seller of the relevant processors. Defendant knew or had reason to know of the specific use for which its processors were purchased or leased.

69. Defendant is and at all relevant times was a "merchant" and seller of "goods" (*i.e.*, Intel processors) as defined under the Uniform Commercial Code.

70. Intel processors are and were at all relevant times "goods" within the meaning of the Uniform Commercial Code.

71. Pursuant to U.C.C. § 2-314, an implied warranty that goods are merchantable is implied in every contract for a sale of goods. Defendant impliedly warranted that its processors were in merchantable condition and fit for the ordinary purpose for which Intel processors are used.

72. Intel processors, when sold or leased and at all times thereafter, were not in merchantable condition and are not fit for the ordinary purpose due to the Defects, and the associated problems and failures caused by the Defects. Thus, Defendant breached its implied warranty of merchantability.

73. As a direct and proximate result of Defendant's breach of its implied warranty of merchantability, Plaintiff and members of the Class have been damaged in an amount to be proven at trial.

74. Defendant cannot disclaim its implied warranties as it knowingly sold or leased a defective product.

75. Defendant was provided notice of the defect by independent research teams, and knew, or should have known, of the existence of the Defects much earlier. Affording Defendant a reasonable opportunity to cure its breach of implied warranties would be unnecessary and futile here because Defendant has known of and concealed the Defects and, on information and belief, has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defects' existence at the time of sale or lease of the processors.

76. Any attempt by Defendant to disclaim or limit the implied warranty of merchantability vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defects. The time limits contained in Defendant's warranty periods were also unconscionable and inadequate to protect Plaintiff and members of the Class. Among other things, Plaintiff and members of the Class did not determine these time limitations, the terms of which unreasonably favored Defendant. A gross disparity in bargaining power existed between Defendant and members of the Class, and Defendant knew or should have known that its processors were defective at the time of sale or lease and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

77. Further, as manufacturers of consumer goods, Defendant is precluded from excluding or modifying an implied warranty of merchantability or limiting customers' remedies for breach of this warranty.

78. Plaintiff and members of the Class have complied with all obligations under the warranty, or otherwise have been excused from performance of said obligations as a result of Defendant's conduct described herein.

79. Defendant's warranties were designed to influence consumers who purchased its processors, including products that contain them.

80. Defendant is estopped by its conduct, as alleged herein, from disclaiming any and all implied warranties with respect to the defective processors.

81. The applicable statute of limitations for the implied warranty claim has been tolled by the discovery rule, concealment, and the terms of the express warranty.

COUNT II

BREACH OF EXPRESS WARRANTY

82. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth herein.

83. Plaintiff brings this count on behalf of itself and members of the Class.

84. Defendant marketed its processors as secure and of particular processing speeds. Such representations formed the basis of the bargain in Plaintiff's and members of the Class's decisions to purchase or lease Intel processors, or devices containing Intel processors.

85. Pursuant to U.C.C. § 2-313, an affirmation of fact, promise, or description made by the seller to the buyer which relates to the goods and becomes a part of the basis of the bargain creates an express warranty that the goods will conform to the affirmation, promise, or description.

86. Defendant is and was at all relevant times a "merchant" and seller of "goods" (*i.e.*, Intel processors) as defined under the Uniform Commercial Code.

87. Intel processors are and were at all relevant times "goods" within the meaning of the Uniform Commercial Code.

88. Defendant represented that its processors were secure and of particular processing speeds. Intel processors were not secure—given that they were subject to the Meltdown and Spectre Defects—and did not operate at stated processing speeds given that patches necessary to mitigate the Defects resulted in reduced processing performance.

89. Plaintiff and members of the Class experienced the existence of the Defects in Intel processors within the warranty periods but had no knowledge of the existence of the Defects, which was known and concealed by Defendant.

90. Plaintiff and members of the Class could not have reasonably discovered the Defects in Intel processors prior to the public disclosure of the Defects by cybersecurity experts or prior to experiencing a known security hack resulting from the Defects.

91. Defendant breached the express warranty by selling Intel processors that were defective with respect to design, workmanship, and manufacture when Defendant knew its processors

were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

92. Intel processors were not of merchantable quality and were unfit for the ordinary purposes for which Intel processors are used because of the existence of the Defects, and do not perform as warranted.

93. Defendant was provided notice of the defect by independent research teams, and knew, or should have known, of the existence of the Defects much earlier. Affording Defendant a reasonable opportunity to cure its breach of express warranties would be unnecessary and futile here because Defendant has known of and concealed the Defects and, on information and belief, has refused to adequately repair or replace its processors free of charge within or outside of the warranty periods despite the Defects' existence at the time of sale or lease of the processors.

94. Any attempt by Defendant to disclaim or limit the express warranties vis-à-vis consumers is unconscionable and unenforceable here. Specifically, any warranty limitation is unenforceable because Defendant knowingly sold or leased a defective product without informing customers about the Defects. The time limits contained in Defendant's warranty periods were also unconscionable and inadequate to protect Plaintiff and members of the Class. Among other things, Plaintiff and members of the Class did not determine these time limitations, the terms of which unreasonably favored Defendant. A gross disparity in bargaining power existed between Defendant and members of the Class, and Defendant knew or should have known that its processors were defective at the time of sale or lease and that its processors were defective and posed security vulnerabilities that, if mitigated, resulted in reduced processing performance.

95. Defendant knew that its processors were inherently defective and did not conform to their warranties and Plaintiff and members of the Class were induced into purchasing or leasing Intel processors, or devices containing Intel processors, under false pretenses.

96. Plaintiff and members of the Class have been excused from performance of any warranty obligations as a result of Defendant's conduct described herein.

97. As a direct and proximate result of Defendant's breach of express warranties, Plaintiff and members of the Class have been damaged in an amount to be determined at trial, including, but

not limited to, repair and replacement costs, monetary losses associated with reduced processor speeds, diminished value of their computer devices, and loss of use of or access to their computer devices.

COUNT III

NEGLIGENCE

98. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth herein.

99. Plaintiff brings this count on behalf of itself and the Class.

100. Defendant owed a duty of care to Plaintiff and members of the Class, arising from the sensitivity of information stored on computers and the foreseeability of the impact of the Defects on data security, to exercise reasonable care in safeguarding sensitive information.

101. Defendant also had a duty to ensure that its processors would function at the quality and processing speeds that it represented to customers, including Plaintiff and members of the Class. This duty included, *inter alia*, designing, maintaining, monitoring, and testing its processors to ensure that members of the Class's data and computers were adequately secured and that its processors would function as promised.

102. Defendant owed a duty to Plaintiff and members of the Class to implement processes that would detect major security vulnerabilities, such as the Defects, in a timely manner.

103. Defendant also owed a duty to disclose the material fact that its processors were defective.

104. But for Defendant's breach of its duties, Plaintiff and members of the Class would not have purchased or leased—or would have paid substantially less for—Intel processors (or devices containing Intel processors) had they known of the Defects and the reduction in processing performance associated with efforts necessary to mitigate the substantial security risks presented by the Defects.

105. Plaintiff and members of the Class were foreseeable victims of Defendant's wrongdoing, and Defendant knew, or should have known, that its processors would cause damages to Plaintiff and members of the Class.

106. As a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class have been damaged in an amount to be proven at trial, including, but not limited to, compensatory damages, incidental and consequential damages, and other damages allowed by law.

COUNT IV

UNJUST ENRICHMENT

107. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth herein.

108. Plaintiff brings this count on behalf of itself and members of the Class.

109. Plaintiff and members of the Class conferred a benefit on Defendant by purchasing or leasing Intel processors, or devices containing Intel processors. Defendant was and should have been reasonably expected to provide its processors free from the Defects.

110. Defendant unjustly profited from the sale and lease of Intel processors, or devices containing Intel processors, at inflated prices as a result of its materially deceptive advertising, marketing, false representations, omissions, and concealment of the Defects in its processors.

111. As a proximate result of Defendant's materially deceptive advertising, marketing, false representations, omissions, and concealment of the Defects, and as a result of Defendant's ill-gotten gains, benefits, and profits, Defendant has been unjustly enriched at the expense of Plaintiff and members of the Class because Intel processors did not provide the represented benefits. It would be inequitable for Defendant to retain its ill-gotten profits without paying the value thereof to Plaintiff and members of the Class.

112. There is privity between Defendant and Plaintiff and members of the Class because Defendant intended customers, such as Plaintiff and members of the Class, to be the purchasers or lessors of Intel processors, or devices containing Intel processors.

113. Plaintiff and members of the Class are entitled to restitution of the amount of Defendant's ill-gotten gains, benefits, and profits, including interest, resulting from their unlawful, unjust, and inequitable conduct.

114. Plaintiff and members of the Class seek an order requiring Defendant to disgorge its gains and profits to Plaintiff and members of the Class, together with interest, in a manner to be determined by the Court.

COUNT V

VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW

CALIFORNIA BUSINESS & PROFESSIONS CODE § 17200, *ET SEQ.*

115. Plaintiff incorporates and realleges each preceding paragraph as though fully set forth herein.

116. Plaintiff brings this count on behalf of itself and members of the Class.

117. California Business & Professions Code § 17200, *et seq.* (the "UCL") prohibits "any unlawful, unfair or fraudulent business act or practice."

118. At all relevant times, Defendant has maintained substantial operations in, regularly conducted business throughout, and engaged in the conduct described herein within the State of California.

119. Defendant, in connection with the Defects, has engaged in unfair, unlawful, and fraudulent business acts and practices in violation of the UCL in that: (1) Defendant's conduct is immoral, unethical, oppressive, unconscionable, and substantially harmful to Plaintiff and members of the Class; (2) any justification for Defendant's conduct would be outweighed by the gravity of the injury to Plaintiff and members of the Class; (3) Defendant's conduct violates the common law; and (4) Defendant's conduct deceived and defrauded Plaintiff and members of the Class.

120. Defendant's unfair, unlawful, and fraudulent business practices were likely to deceive a reasonable consumer. Plaintiff and members of the Class used Defendant's products and had business dealings with Defendant either directly or indirectly through third-parties, and were the intended recipients of Defendant's processors.

121. As a result of Defendant's systematic unlawful, unfair, and fraudulent conduct, Plaintiff and members of the Class have been injured. The harm caused by this conduct vastly outweighs any legitimate business utility it possibly could have. Plaintiff and members of the Class

are entitled to restitution, including disgorgement of profits, costs, and attorneys' fees in amounts to be determined at trial.

122. Defendant's conduct is or may well be continuing and ongoing. Accordingly, Plaintiff and members of the Class are entitled to injunctive relief to prohibit or correct such ongoing acts of unfair competition, in addition to obtaining equitable monetary relief.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of itself and all others similarly situated, respectfully request that this Court enter judgment against Defendant and in favor of Plaintiff and the Class, and award the following relief:

A. An order certifying this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, declaring Plaintiff as the representative of the Class, and Plaintiff's counsel as counsel for the Class;

B. An order awarding declaratory relief and enjoining Defendant from continuing the unlawful, deceptive, harmful, and unfair business conduct and practices alleged herein;

C. Appropriate injunctive and equitable relief;

D. A declaration that Defendant is financially responsible for all Class notice and the administration of Class relief;

E. Costs, restitution, damages, including statutory and punitive damages, penalties, and disgorgement in an amount to be determined at trial;

F. An order requiring Defendant to pay both pre- and post-judgment interest on any amounts awarded;

G. An award of costs and attorneys' fees; and

H. Such other or further relief as the Court may deem appropriate, just, and equitable.

IX. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury.

DATED: January 12, 2018

Respectfully submitted,

KESSLER TOPAZ MELTZER & CHECK, LLP

/s/ Eli R. Greenstein
ELI R. GREENSTEIN (Bar No. 217945)
egreenstein@ktmc.com
JENNIFER L. JOOST (Bar No. 296164)
jjoost@ktmc.com
STACEY M. KAPLAN (Bar No. 241989)
skaplan@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Tel: (415) 400-3000
Fax: (415) 400-3001

-and-

JOSEPH H. MELTZER
jmeltzer@ktmc.com
SAMANTHA HOLBROOK
sholbrook@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Tel: (610) 667-7706
Fax: (610) 667-7056

Attorneys for Plaintiff Zog, Inc.